U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371***		*Attorney's Docket Number* JEK/Lamla
		U.S. Application Number (if known) 09/486723
International Application Number PCT/EP98/05669	*International Filing Date* 07 September 1998	*Priority Date Claimed* 09 September 1997
Title of Invention METHOD FOR TESTING THE AUTHENTICITY OF A DATA CARRIER		
Applicant(s) for DO/EO/US Michael LAMLA et al.		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.
2. □ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.
3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. □ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. □ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. □ A translation of the International Application into English *(35 USC 371(c)(2))*.
7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. □ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ have been transmitted by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. □ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.
9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. (□ Executed ☒ Unexecuted)
10. □ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

Items 11 to 16 below concern other document(s) or information included:

11. □ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.
12. □ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.
13. ☒ A **FIRST** preliminary amendment.
    □ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. □ A substitute specification.
15. □ A change of power of attorney and/or address letter.
16. □ Other items or information:
    2 sheets of drawings

Application Number (if Known)	*International Application Number*	*Attorney's Docket Number*
09/486723	PCT/EP98/05669	JEK/Lamla

				Calculations	PTO USE ONLY
17. The following fees are submitted: **Basic National Fee** *(37 CFR 1.492(a)(1)-(5))*: ☒ Search report has been prepared by the EPO or JPO .... $840.00 □ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* ..... $670.00 □ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* .... $690.00 □ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO .... $970.00 □ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) $96.00					
ENTER APPROPRIATE BASIC FEE AMOUNT				$ 840.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.					
CLAIMS	**NUMBER FILED**	**NUMBER EXTRA**	**RATE**		
Total Claims	14 -20 =		× $18.00		
Independent Claims	4 -3 =	1	× $78.00	$ 78.00	
Multiple Dependent Claims (if applicable)			+ $260.00		
TOTAL OF ABOVE CALCULATIONS				$ 918.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity Statements must also be filed (Note *37 CFR 1.9, 1.27, 1.28)*					
SUBTOTAL				$ 918.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.					
TOTAL NATIONAL FEE				$ 918.00	
Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property.					
TOTAL FEES ENCLOSED				$ 918.00	
			Amount to be:	Refunded:	
				Charged:	

a. ☒ A check in the amount of $918.00 to cover the fees is enclosed.

b. □ Please charge my **Deposit Account Number 02-0200** in the amount of $ ______ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 09 March 2000

Respectfully submitted,

J. Ernest Kenney

J. ERNEST KENNEY
Attorney for Applicant
Registration Number: 19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Patent Application
No. PCT/EP98/05669

PCT/DO/EO/US

International Filing Date: 07 September 1998

Applicant: Michael LAMLA et al.

For: METHOD FOR TESTING THE AUTHENTICITY OF A DATA CARRIER

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application.

The claims were not amended during the international phase. Before calculation of the filing fee and before examination, please amend the application as follows:

IN THE CLAIMS:

Please amend the original as-filed claims as follows:

Claim 4, line 1; change "either of claims 2 to 3" to --claim 2--;

Claim 5, line 1; change "either of claims 2 to 3" to --claim 2--;

Claim 6, line 1; change "any of claims 2 to 5" to --claim 2--;

Claim 7, line 1; change "any of claims 1 to 6" to --claim 1--;

Claim 11, line 1; change "any of claims 1 to 10" to --claim 1--;

REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to correct any improper multiple dependent claims. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. ERNEST KENNEY
Attorney for Applicant
Registration Number 19,179

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: March 9, 2000

S:\Producer\jek\LAMLA - pct05669\preliminary amendment.wpd

A method for testing the authenticity of a data carrier

This invention relates to a method for testing the authenticity of a data carrier according to the preamble of claim 1. The invention further relates to the data carrier used in said method and to a system comprising the data carrier and an external device.

To prevent unauthorized production and replication of data carriers or the use of such data carriers, it is necessary to be able to test the authenticity of a data carrier with a high measure of reliability. It is also necessary in many cases to be able to test the authenticity of an external device communicating with the data carrier.

A method for testing the authenticity of a data carrier is known from DE 44 19 805 A1. In the known method the data carrier used has at least one integrated circuit with memory units and logical units and a data line for data exchange with an external device. The integrated circuit additionally has a separate hardwired circuit for transmitting and/or receiving data during the power-up sequence. Said separate circuit is used for authenticity testing, the first transmission or reception of data being completed within a defined time domain of the power-up sequence in which no defined state is specified for the data line by ISO standard 7816. Data relevant for authenticity testing are transmitted between data carrier and external device either via a data line on which other data are also exchanged between data carrier and external device or via other lines which do not meet this standard data line and are currently reserved for future applications.

The problem of the invention is to state a method for testing the authenticity of a data carrier and/or an external device which can be used flexibly and simultaneously offers a very high security standard.

This problem is solved by the features stated in the independent claims.

The basic idea of the invention is to equip the data carrier and external device each with a special additional apparatus for generating and/or testing authenticity data and to perform the data transmission between data carrier and external device necessary for authenticity testing at least partly via a special transmission channel, the additional apparatuses for generating and/or testing the authenticity data and optionally also the transmission channel making special demands on the data carrier or external device which cannot be met by conventional designs.

The invention has the advantage of permitting very reliable authenticity testing without using the standard transmission channel between data carrier and external device or being dependent on the standard transmission channel.

Further, the invention offers very good protection from impermissible reproduction of the data carrier or external device since the inventive additional apparatuses for generating and/or testing authenticity data and the inventive additional transmission channel for authenticity testing are not present in conventional data carriers and external devices, thereby making it difficult for unauthorized persons to procure the required components. This hurdle for impermissible reproduction can be made even higher if the additional apparatuses for generating and/or testing authenticity data and the transmission channel for authenticity testing presuppose a technology in the data carrier or external device which can be procured only with great difficulty or not at all by an unauthorized person. This technology preferably resides at least partly in a different technical area from the technologies required for producing conventional data carriers.

In authenticity testing of the data carrier the additional apparatus of the data carrier generates authenticity data and communicates them to the external device via the specially provided transmission channel. The external device tests the communicated authenticity data and decides on the authenticity of the data carrier. This decision can additionally be made contingent on whether a connection exists between the additional apparatus of the data carrier and a microcontroller disposed in the data carrier.

Depending on security requirements and special circumstances of the application, one performs the data transmission necessary for authenticity testing using at least one transmission channel separated either logically or physically from the standard transmission channel.

Logical separation can be attained for example by using the same line or transmission path for transmitting authenticity data as for transmitting other data but coding authenticity data on this line or transmission path in such a way that they can be separated from other data and do not impair transmission of other data. For coding authenticity data one can use tolerances permitted by the ISO standard for voltage level or for localization in time of the transition between different logic levels of the signals of the standard transmission channel. Since this kind of coding does not exceed tolerances specified by the ISO standard for voltage levels or transitional behavior of the signals, this kind of data transmission is ISO-compatible. For applications outside the ISO standard the stated tolerance ranges can be exceeded. An advantage of the described data transmission is in addition that one can fall back on existing lines and thus need not install additional lines or other transmission paths. Instead of the line of the standard transmission channel one can also fall back on other lines, for example the line for the supply voltage or the line for the clock signal or also a contactless transmission path. The only important thing is that the line or transmission path used permits a connection to be made between data carrier and external device for the purpose of transmitting authenticity data.

However, physical separation of the transmission channel for transmitting authenticity data from the standard transmission channel has the advantage of opening up almost unlimited possibilities of variation for realizing the authenticity testing method. This permits technical effort and thus also costs, on the one hand, and the desired security standard, on the other hand, to be optimally adapted to the particular application. Since compatibility with an existing line or transmission path can be disregarded, one can use for example a highly complex and limitedly available additional apparatus of any construction for generating the data to be transmitted which identifies the data carrier or external device as authentic and thus makes it virtually impossible to imitate these components. For example, one can also use a great variety of contactless transmission techniques in this connection.

Further advantageous embodiments and developments are described in the following and shown in the drawings, in which:

Fig. 1 shows a block diagram to illustrate the basic principle of the invention,

Fig. 2 shows a variant of the block diagram of Fig. 1,

Figs. 3*a* and 3*b* show block diagrams of embodiments of the inventive systems wherein authenticity data are transmitted via the standard data line, Figs. 4*a* and 4*b* show signal patterns over time on the standard data line in case authenticity data are transmitted within transition regions defined in the area of the signal edges of standard data,

Figs. 5*a* and 5*b* show signal patterns over time on the standard data line in case authenticity data are impressed on the signal for standard data as small voltage fluctuations, and

Fig. 6 shows a block diagram of an embodiment of the inventive system wherein data required for authenticity testing are transmitted contactlessly between external device and data carrier.

Fig. 1 shows a block diagram to illustrate the basic principle of the invention. Chip card 1 has microcontroller 3 and additional apparatus 4 for generating and testing authenticity data. Microcontroller 3 of chip card 1 is connected with microcontroller 2 of external device 5 via first transmission channel *A*, which normally corresponds to the standard data line. Transmission channel *A* and also further transmission channels are shown by double arrows indicating the direction of data transmission. Via transmission channel *A* transactions are completed in known fashion between chip card 1 and external device 2, which may be for example a POS terminal or an automatic teller machine, etc. Data transmission via transmission channel *A* follows a transmission protocol defined by ISO standard 7816. In known systems the complete authenticity testing of chip card 1 or external device 2 - if necessary for the particular application - is also performed via transmission channel *A*. This authenticity testing can be performed for example in the form of a reciprocal authentication method on the challenge and response principle.

According to the invention, further transmission channel *B* is present in addition to transmission channel *A* for connecting additional apparatus 4 of chip card 1 with additional apparatus 6 of external device 2. Further, microcontrollers 3, 5 and additional apparatuses 4, 6 are interconnected, respectively. Data required by chip card 1 or external device 2 for authenticity testing which were previously generated by additional apparatus 4 or 6 are transmitted via transmission channel *B*. Authenticity data received by other additional apparatus 6 or 4 are evaluated and it is decided whether chip card 1 or the external device is authentic. Additional apparatus 4 of chip card 1 can be part of the module bearing microcontroller 3. Additional apparatus 6 of external device 2 will normally be realized as a separate module, referred to as a secure application module (abbreviated as SAM) and executed in the form of a chip card.

The method for testing the authenticity of chip card 1 by external device 2 can take place as follows.

External device 2 communicates input data, for example a random number, to chip card 1 via transmission channel *B*. Additional apparatus 4 of chip card 1 uses the input data to generate authenticity data and communicates the authenticity data to external device 2 via transmission channel *B*. External device 2 receives the authenticity data and decides on the authenticity of chip card 1 on the basis of the received authenticity data by means of additional apparatus 6.

The described method can be modified insofar as authenticity data can be generated by additional apparatus 4 of chip card 1 without input data from external device 2, or generation of authenticity data can already be begun before the input data are completely transmitted. Further modifications can be to transmit the input data or authenticity data via transmission channel *A*. A plurality of different methods can be used for generating the authenticity data. For example the authenticity data can be calculated from the input data or the authenticity data can be generated by exploiting special physical effects, optionally in accordance with material properties of the additional apparatus. The important thing in all methods for generating the authenticity data is that the latter cannot be simulated by unauthorized third parties with apparatuses having the outer dimensions of chip card 1. Such simulation could be, if the authenticity data are calculated, to implement the algorithm processed by additional apparatus 4 on a powerful computer. In order to prevent this one should design additional apparatus 4 so that its computing power is far above that attainable with available microcontrollers.

In the variant of the invention shown in Fig. 1, both transmission channel *A* and transmission channel *B* permit bidirectional data exchange, i.e. data exchange from chip card 1 to external device 2 and data exchange from external device 2 to chip card 1. The separation between transmission channel *A* and transmission channel *B* can be of either a physical or a logical nature. With physical separation of the transmission channels one selects for transmission channel B a separate transmission path completely independent from transmission channel A. One can thus for example provide an additional line between chip card 1 and external device 2, or contactless transmission can take place between chip card 1 and external device 2 which is independent from standard data transmission via transmission channel A. With logical separation of transmission channels A and B, transmission channels A and B are physically one and the same transmission channel, i.e. one and the same line or one and the same contactless transmission path. However, one uses for data transmission different signals which can be separated from each other by chip card 1 or terminal 2.

Fig. 2 shows a block diagram of a form of the invention somewhat modified over Fig. 1. Chip card 1 and the external device are again interconnected via bidirectional line A used for standard data exchange. This line is a realization of transmission channel A in case chip card 1 is a contact-type chip card. If contactless chip card 1 is to be used instead, transmission channel A is not realized in the form of a line but by a contactless transmission path via which data are transmitted for example as electromagnetic, electrostatic, magnetic, acoustic or optical signals. This different design of transmission channel A is also applicable in the form of the invention shown in Fig. 1. In contrast to Fig. 1, data required for authenticity testing are communicated via two separate transmission channels B_1 and B_2 according to Fig. 2. Transmission channel B_1 is used for data transmission from external device 2 to chip card 1 and transmission channel B_2 for data transmission in the reverse direction. Transmission channels B_1 and B_2 can be separated either logically or physically from each other and from transmission channel A.

In a development of the invention, one of transmission channels B_1 or B_2 can be identical with transmission channel A, i.e. authenticity data or data required for authenticity testing can be transmitted partly via transmission channel A. In all embodiments of the invention it is fundamentally possible to integrate transmission channel A into the authenticity testing method, i.e. communicate part of the data transmitted in this method via transmission channel A.

Division of the transmission channel for data required for authenticity testing into transmission channels B_1 and B_2 as shown in Fig. 2 can be necessary in particular when the signals formed by chip card 1 and external device 2 in the authenticity testing method are so different physically that transmission via the same channel is impossible. This may be the case for example when only the authenticity of chip card 1 is to be tested and chip card 1 emits for authenticity testing special electromagnetic signals which can be generated only with authentic additional apparatus 4. The electromagnetic signals are then communicated via transmission channel B_2, and control signals influencing the generation of the electromagnetic signals can be transmitted from external device 2 to chip card 1 via transmission channel B_1.

Fig. 3*a* shows a block diagram for an embodiment of the invention wherein data required for authenticity testing are transmitted between chip card 1 and external device 2 via the standard data line, i.e. transmission channel *A* for standard data and transmission channel *B* for authenticity data are bound to the same line so that the separation between channels *A* and *B* is not physical but only logical. Unlike Figs. 1 and 2, Fig. 3*a* does not show transmission channels *A* and *B* themselves but rather a realization of the channels in the form of the standard data line. In order to ensure differentiation from the representation of the transmission channels, the lines or transmission paths are shown as simple arrows. It is stated in parentheses which transmission channels are realized by the particular line or transmission path.

Within chip card 1 microcontroller 3 and additional apparatus 4 are connected with the standard data line. Further, microcontroller 3 and additional apparatus 4 are interconnected. Logical separation of transmission channels *A* and *B* is effected by microcontroller 3 and additional apparatus 4, which executes essential parts of the authenticity testing method, each filtering out the signals relevant for them or subjecting the standard data line to the signals generated by them. If this should be necessary, synchronization or data exchange is possible via the connecting line between microcontroller 3 and additional apparatus 4.

External device 2 can be constructed in a similar way to chip card 1 and contain microcontroller 5 and additional apparatus 6 which are connected with the standard data line and with each other. The system shown in Fig. 3*a* can transmit data required for authenticity testing in a digital form via the standard data line. A signal pattern possible in this connection is shown in Fig. 4*a* and described in the corresponding text.

Fig. 3*b* shows a block diagram of an embodiment of the inventive system wherein data required for authenticity testing are transmitted in the form of digital or analog signals via the standard data line. As in Fig. 3*a*, transmission channels *A* and *B* for standard data and authenticity data are again separated not physically but only logically. On the part of chip card 1 the logical separation of transmission channels *A* and *B* is effected by mixing/demixing module 7 which splits signals from the standard data line into standard data signals and authenticity data signals or brings together signals for standard data and signals for authenticity data for transmission via the standard data line. For this purpose, mixing/demixing module 7 is connected with the standard data line, on the one hand, and with microcontroller 3 and additional apparatus 4, on the other hand. Further, microcontroller 3 and additional apparatus 4 are interconnected. External device 2 is constructed analogously and likewise has mixing/demixing module 8 connected with the standard data line and with microcontroller 5 and additional apparatus 6. In external device 2 microcontroller 5 and additional apparatus 6 are also interconnected. The system shown in Fig. 3*b* can process not only the analog signal patterns shown in Figs. 4*b* and 5*b* but also the digital signal patterns shown in Figs. 4*a* and 5*a*.

Fig. 4*a* shows a signal pattern on the standard data line of the system shown in Fig. 3*a*. The signal level is shown as a function of time *t*. The standard data line transmits both the dashed-line signals of transmission channel *A*, i.e. standard data, and the signals of transmission channel *B* shown in the form of continuous lines, i.e. authenticity data. Since transmission of standard data via the standard data line is defined by ISO standard 7816 and transmission of authenticity data is to be effected in conformity with ISO without impairing the standard data and at high speed, one has used transition regions *TZ* defined in the ISO standard which are disposed at the beginning and end of each data signal and within which the signal is not scanned and evaluated. The signal pattern within the transition regions thus has no influence on the evaluation of the signal according to ISO standard 7816 and can be used for transmitting authenticity data. For this purpose, the authenticity data are modulated upon the signal for the standard data by means of a suitable modulation method, e.g. amplitude modulation, frequency modulation, pulse-coded modulation, etc. For scanning and evaluating the authenticity data one then of course requires an additional device since a chip card designed solely by the ISO standard would overlook authenticity data contained in the transition regions. Thus, additional apparatus 4 not present in conventional chip cards is already required for reading the authenticity data, which considerably impedes unauthorized reproduction of inventive chip card 1. Additional apparatus 4, which is not present in standard chip cards, is also necessary for transmitting authenticity data within the transition region and ultimately also for generating authenticity data. Corresponding additional apparatus 6 is also required in external device 2. One thus attains a very high security level altogether.

Fig. 4*b* shows a signal pattern over time on the standard data line which differs from the pattern shown in Fig. 4*a* in that authenticity data are transmitted as analog signals. Otherwise the signal pattern in Fig. 4*b* meets the same criteria as underlie Fig. 4*a*, i.e. authenticity data are communicated within transition regions *TZ* of standard data and one can use the modulation methods stated for Fig. 4*a*. Processing of the signals shown in Fig. 4*b* is effected using the system according to Fig. 3*b*. The system shown in Fig. 3*a* is unsuitable since mixing/demixing modules 7 and 8 shown in Fig. 3*b* are required for separating and bringing together signals for authenticity data and signals for standard data. The use of analog signals for data transmission impedes unauthorized reproduction of chip card 1 or external device 2 even further since this requires additional know-how for integrating the required analog technology into chip card 1. The knowledge of digital technology required for constructing conventional chip cards is insufficient alone.

Fig. 5*a* shows the signal pattern on the standard line for a variant of logical separation of transmission channels *A* and *B*. The signal for standard data is dashed, the signal for authenticity data is continuous. In this embodiment, tolerance *T* permitted by ISO standard 7816 for the signal level of standard data is used for transmitting authenticity data. For this purpose the authenticity signal is superimposed on the standard data signal, the level of the authenticity signal being within the permissible tolerance range of the signal for standard data. One must make sure that the actually occurring level fluctuations of the standard data signal together with the superimposed authenticity signal do not cause tolerance range *T* to be exceeded. Besides the standard data signal, the basic signal for superimposition selected can be any signal, e.g. the clock signal or the signal for the operating voltage. In all cases authenticity data can be transmitted via existing lines or transmission paths, the signals transmitted via the same line or transmission path being separated only logically.

Fig. 5*b* shows the time behavior of signals meeting similar conditions to the signals according to Fig. 5*a*. The main difference over Fig. 5*a* is that authenticity data are transmitted by means of analog signals, i.e. in contrast to Fig. 5*a* the originally existing signal is superimposed not by a digital signal but by an analog signal, tolerance range *T* also being taken into account here. Like the signal pattern according to Fig. 5*a*, the signal pattern according to Fig. 5*b* is processed or generated with the system shown in Fig. 3*b*. Mixer/demixer 3, 8 is again used for superimposing and separating the analog or digital authenticity signal and the originally existing signal.

The modulation methods described for Fig. 4*a* can also be used in the embodiments according to Figs. 5*a* and 5*b*.

Fig. 6 shows a block diagram of a variant of the inventive system wherein transmission channels *A* for standard data and *B* for authenticity data are physically separated, standard data being transmitted via a line and authenticity data contactlessly using two transceivers 9 and 10. Transceivers 9 and 10 are each connected with one of additional apparatuses 4 and 6. Additional apparatus 4 of chip card 1 is further connected with microcontroller 3 connected to the standard data line (transmission channel *A*). Additional apparatus 6 of the external device is also connected with microcontroller 5 again connected to the standard data line. Contactless data transmission between transceivers 9 and 10 can be realized in different ways. For example, one can use forms of transmission customary in the area of chip card technology via electromagnetic waves, magnetic or electric fields and light in the visible or invisible range. If an especially high security standard is to be attained, one selects the form of transmission so that it cannot be performed with conventional chip cards but necessitates special hardware. In this connection one can improve the security standard even further if the additionally required hardware presupposes a very high measure of know-how, is inaccessible to an unauthorized third party and/or can be realized only with complex and costly equipment. For example, one can use for transmission radiation-induced luminescence or electroluminescence of a suitable material. It is also expedient to dispose the luminescent material on the chip card in a special pattern in order to impede reproduction further. One can also use a certain spatial arrangement of different receivers and transmitters so that reproduction from discrete components is extremely difficult. One can likewise use luminescent materials which are very hard to procure, and to mislead an unauthorized third party one can use a mixture of wavelengths for data transmission, the information being contained only in a single wavelength or having to be combined from information portions scattered over different wavelengths, etc.

A further variant of data transmission is to subject chip card 1 to a high-frequency pulse whereupon chip card 1 modulates the high-frequency pulse and sends it back to the external device.

In all variants, reproduction or manipulation of chip card 1 or external device 2 can also be impeded if additional apparatus 4, 6 is coupled to microcontroller 3, 5 and works properly only if this connection actually exists. This coupling impedes imitation of additional apparatus 4, 6 by means of discrete components when microcontroller 3, 5 offers no simple possibility of external coupling.

Chip card 1 can be executed as a contact-type chip card wherein standard data are transmitted via one or more contact surfaces. Chip card 1 can also be executed as a contactless chip card wherein standard data are transmitted contactlessly.

Patent claims

1. A method for testing the authenticity of a data carrier (1) having an integrated circuit by an external device (2) with which the data carrier (1) exchanges data, comprising the steps of:
   - providing a first transmission channel (*A*) for transmitting signals between the data carrier (1) and the external device (2),
   - providing a second transmission channel (*B*) logically separated from the first transmission channel (*A*), the separation of the first and second transmission channels being so designed that data transmission via one transmission channel does not interfere with data transmission via the other transmission channel and the second transmission channel (*B*) is activable during the total time period between activation and deactivation of the data carrier (1),
   - having the data carrier (1) generate a signal required for authenticity testing,
   - transmitting the signal for authenticity testing from the data carrier (1) to the external device (2) or a signal required for generating the signal for authenticity testing from the external device (2) to the data carrier (1) at least partly via the second transmission channel, and
   - having the external device (2) receive the signal for authenticity testing, and deciding on the basis of the received signal whether the data carrier (1) is authentic.
2. A method according to claim 1, characterized in that the second transmission channel (*B*) is provided by modulating the signal of the first transmission channel.
3. A method according to claim 2, characterized in that modulation does not impair an ISO compatibility of data exchange between the data carrier (1) and the external device (2) existing for the first transmission channel (*A*).

4. A method according to either of claims 2 to 3, characterized in that modulation is performed in areas of the signal pattern which are not evaluated according to the ISO standard.

5. A method according to either of claims 2 to 3, characterized in that the changes caused by modulation in the signal of the first transmission channel (*A*) are within the range of variation of the signal level permitted by the ISO standard.

6. A method according to any of claims 2 to 5, characterized in that modulation and demodulation of the signal are performed in the data carrier (1) and in the external device (2) with the aid of a mixing/demixing device (7, 8) in each case.

7. A method according to any of claims 1 to 6, characterized in that the first transmission channel (*A*) is a line for transmitting standard data or a line for transmitting the clock signal or a line for the supply voltage.

8. A method for testing the authenticity of a data carrier (1) having an integrated circuit (3) by an external device (2) with which the data carrier (1) exchanges data, comprising the steps of:

- providing a first transmission channel (*A*) for transmitting signals between the data carrier (1) and the external device (2),
- providing a second transmission channel (*B*) physically separated from the first transmission channel (*A*) and comprising at least one line or contactless transmission path not provided according to the ISO standard, the second transmission channel (*B*) being activable during the total time period between activation and deactivation of the data carrier (1),
- having the data carrier (1) generate a signal required for authenticity testing,
- transmitting the signal for authenticity testing from the data carrier (1) to the external device (2) or a signal required for generating said signal from the external device (2) to the data carrier (1) at least partly via the second transmission channel (*B*), and

- having the external device (2) receive the signal for authenticity testing, and deciding on the basis of the received signal whether the data carrier (1) is authentic.

9. A method according to claim 8, characterized in that the contactless transmission path is realized by transmitting the data as electromagnetic, electrostatic, magnetic, acoustic or optical signals.

10. A method according to claim 9, characterized in that a mixture of wavelengths is used for transmission via the contactless transmission path.

11. A method according to any of claims 1 to 10, characterized in that the decision on authenticity of the data carrier (1) is contingent on whether data exchange is possible between the devices (3, 4) to which the first and second transmission channels are coupled in the data carrier (1).

12. A data carrier (1) which can exchange data with an external device (2) and has an integrated circuit, wherein

    - the data carrier (1) has a first device (3) for generating signals for data exchange between the data carrier (1) and the external device (2), and the first device (3) is adapted to be coupled to a first transmission channel (*A*),
    - the data carrier (1) has a second device (4) for generating signals required for authenticity testing of the data carrier (1), and the second device (4) is adapted to be coupled to a second transmission channel (*B*) and connected with the first device (3),
    - the first and second transmission channels are separated logically or physically, and
    - data exchange with the second device (4) does not interfere with data exchange with the first device (3), and the second device (4) is ready for generating signals for authenticity testing of the data carrier during the total time period between activation and deactivation of the data carrier (1).

13. A data carrier according to claim 12, characterized in that the first device (3) and the second device (4) are each coupled to the transmission channels (*A*, *B*) via a mixing/demixing module (7).

14. A system for testing the authenticity of a data carrier (1) and/or an external device (2) comprising:

- a data carrier (1) with a first device (3) for generating signals for data exchange with the external device (2) and a second device (4) for generating and/or processing signals for authenticity testing,
- an external device (2) with a first device (5) for generating signals for data exchange with the data carrier (1) and a second device (6) for generating and/or processing signals for authenticity testing,
- a first transmission channel (*A*) for transmitting signals between the first device (3) of the data carrier (1) and the first device (5) of the external device (2),
- and a second transmission channel (*B*) for transmitting signals between the second device (4) of the data carrier (1) and the second device (6) of the external device (2), the first and second transmission channels (*A*, *B*) being separated logically or physically and the separation of the first and second transmission channels (*A*, *B*) being so designed that data transmission via one transmission channel does not interfere with data transmission via the other transmission channel, and the second transmission channel (*B*) being activable during the total time period between activation and deactivation of the data carrier (1).

Abstract

The invention relates to a method for testing the authenticity of a data carrier (1) and/or an external device (2) which enters into data exchange with the data carrier (1). According to the invention, the data carrier (1) and the external device (2) are each equipped with a special additional apparatus (4, 6) for generating and/or testing authenticity data. Data transmission between the data carrier (1) and the external device (2) as required for authenticity testing is performed at least partly via a special transmission channel (*B*). The transmission channel (*B*) for transmitting authenticity data is separated physically or logically from a transmission channel (*A*) for transmitting standard data so that there is no mutual interference of data transmission via the two transmission channels (*A*, *B*). In authenticity testing, the additional apparatuses for generating and/or testing authenticity data (4, 6) of the data carrier (1) and external device (2) and optionally also the transmission channel (*B*) for authenticity data must meet special demands which cannot be met by conventional designs. The transmission channel (*B*) for transmitting authenticity data is activable during the total time period between activation and deactivation of the data carrier (1) so that authenticity testing can be performed anytime.

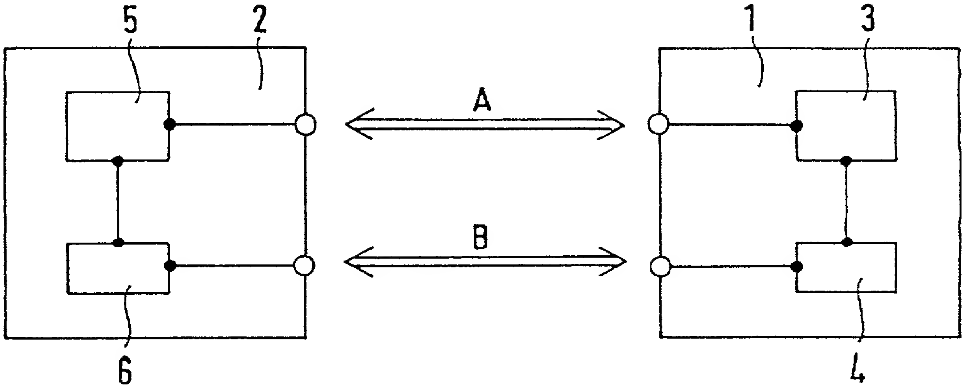

FIG.1

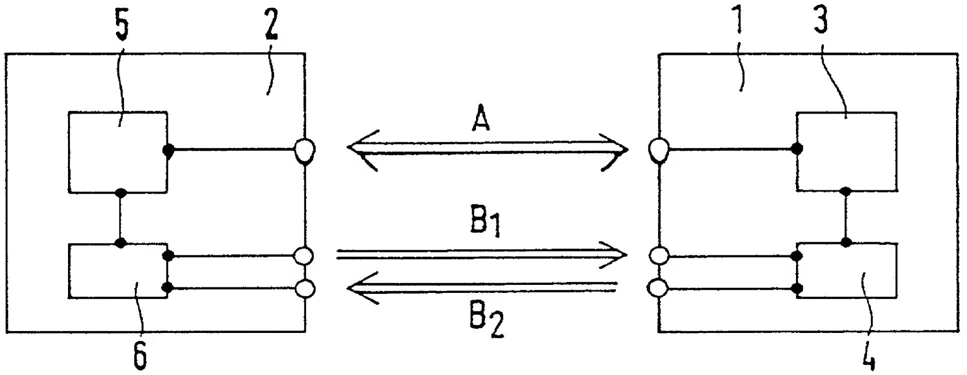

FIG.2

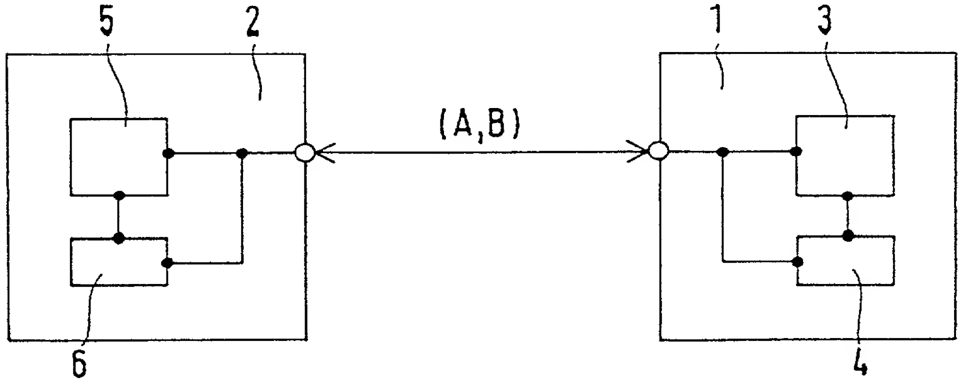

FIG.3a

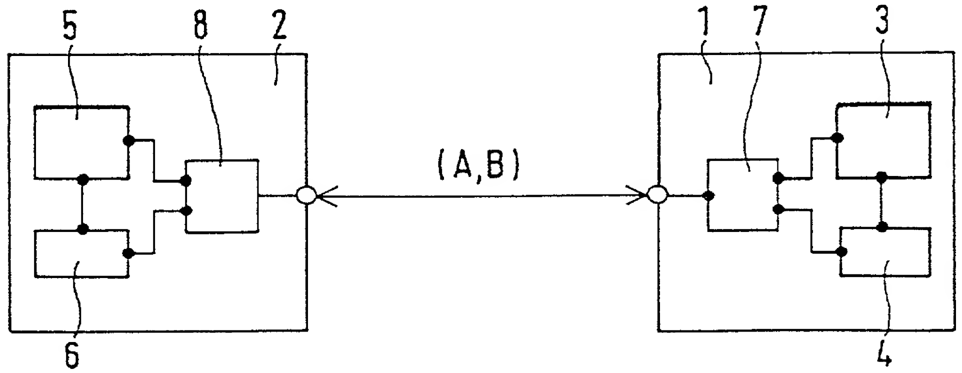

FIG.3b

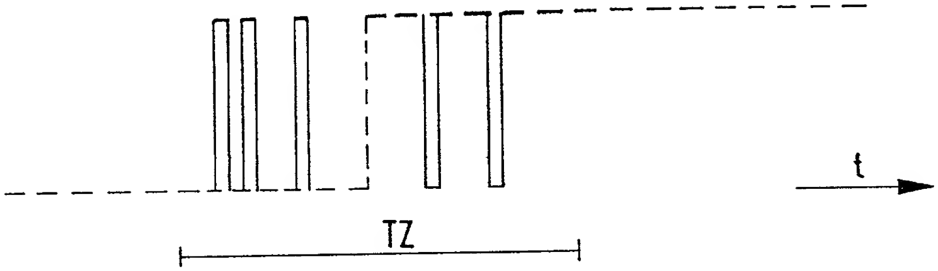

FIG.4a

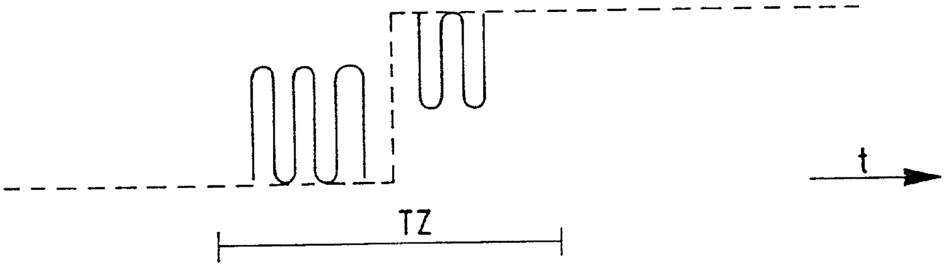

FIG.4b

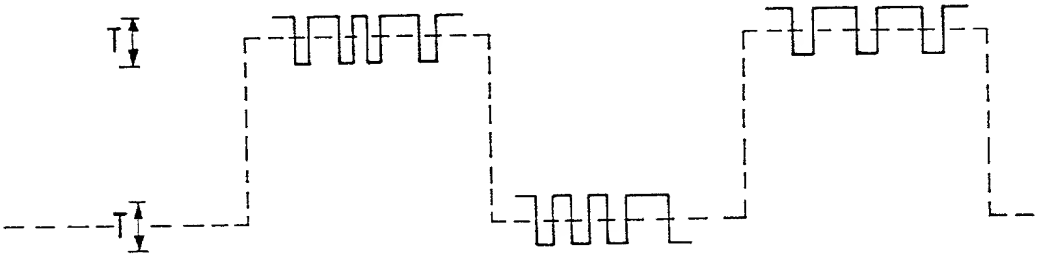

FIG.5a

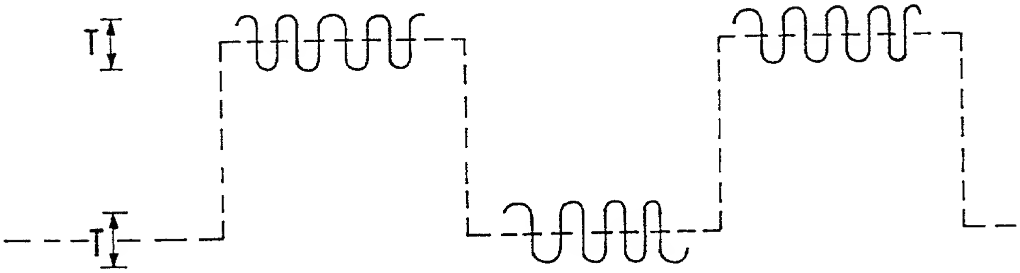

FIG.5b

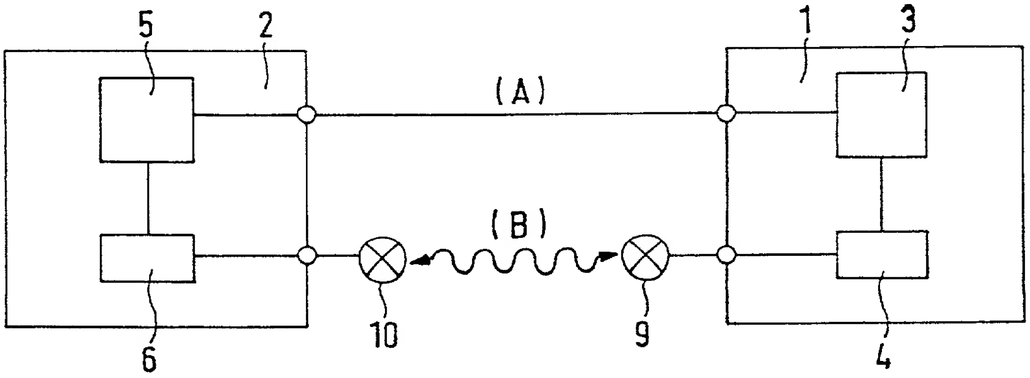

FIG.6

ATTORNEY/DOCKET NO: JEK/Lamla

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:
METHOD FOR TESTING THE AUTHENTICITY OF A DATA CARRIER

the specification of which (check one):

□ is attached hereto, or ☒ was filed on: **07 September 1998** as U.S. Application Number or PCT International Application Number: **09/486,723**

and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56.* I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	**Country**	**Day/Month/Year Filed**	**Yes**	**No**
197 39 448.5	Germany	09 September 1997	X	

□ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	**Day/Month/Year Filed**

□ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

□ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to:
BACON & THOMAS, PLLC
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney (703) 683-0500**

FULL NAME OF FIRST OR SOLE INVENTOR **Michael LAMLA**	CITIZENSHIP **German**
RESIDENCE ADDRESS Krempelhuberplatz 7, D-80935 München, Germany	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 10.04.2000	SIGNATURE

☒ *See following page(s) for additional joint inventors.*

CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

Page 2

PRIOR FOREIGN APPLICATION(S) (35 USC §119)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E)	
Application Number	Day/Month/Year Filed

PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120)		
Application Number	Filing Date	Status - Patented, Pending or Abandoned

200

FULL NAME OF JOINT INVENTOR Hermann DREXLER	CITIZENSHIP German
RESIDENCE ADDRESS Oberländerstr. 5a, D-81371 München, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 18.4.00	SIGNATURE X

300

FULL NAME OF JOINT INVENTOR Wolfgang RANKL	CITIZENSHIP German
RESIDENCE ADDRESS St.-Gunther-Weg 5, D-94258 Frauenau, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 18./IV/2000	SIGNATURE X

400

FULL NAME OF JOINT INVENTOR Franz WEIKMANN	CITIZENSHIP German
RESIDENCE ADDRESS Einsteinstr. 131, D-81675 München, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 2.05.2000	SIGNATURE X

500

FULL NAME OF JOINT INVENTOR Wolfgang EFFING	CITIZENSHIP German
RESIDENCE ADDRESS Siriusstr. 28a, D-82205 Gilching, Germany DEX	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 25.04.2000	SIGNATURE X Wolfgang [illegible]

□ *See following pages for additional joint inventors/priority applications.*